Attachment 1

Department of the Interior

Security Control Standard

Incident Response

April 2011

Version: 1.1

Attachment 1

Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	**Date:**

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 13, 2011	Initial draft
Timothy Brown	0.2	January 20, 2011	Incorporated comments into body text
Timothy Brown	0.21	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes. Retained notes re: “service provider” and/or Joint Authorization Board (JAB)
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

SECURITY CONTROL STANDARD: INCIDENT RESPONSE

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Incident Response (IR) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

IR-1 INCIDENT RESPONSE POLICIES AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Applicability: All Information Systems

Control: The organization:

a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and
b. Provides refresher training at least annually.

Supplemental Guidance: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.

Control Enhancements:

1. The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
2. The organization employs automated mechanisms to provide a more thorough and realistic training environment.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** IR-2	**MOD** IR-2	**HIGH** IR-2 (1) (2)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Applicability: Moderate and High Impact Information Systems

Control: The organization tests and/or exercises the incident response capability for the information system at least annually using tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended) to determine the incident response effectiveness and documents the results.

Supplemental Guidance: None.

Control Enhancements:

1. The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

   Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability. Related control: AT-2.

References: NIST Special Publications 800-84, 800-115.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** IR-3	**HIGH** IR-3 (1)

IR-4 INCIDENT HANDLING

Applicability: All Information Systems

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

1. The organization employs automated mechanisms to support the incident handling process.

   Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1)

IR-5 INCIDENT MONITORING

Applicability: All Information Systems

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Control Enhancements:

1. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

   Enhancement Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-6, AU-7, SI-4.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-5	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Applicability: All Information Systems

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended) ; and
b. Reports security incident information to designated authorities.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5.

Control Enhancements:

1. The organization employs automated mechanisms to assist in the reporting of security incidents.

References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.

Priority and Baseline Allocation:

P1	**LOW** IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Applicability: All Information Systems

Control: The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.

Control Enhancements:

1. The organization employs automated mechanisms to increase the availability of incident response-related information and support.

   Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

2. The organization:

   a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
   b. Identifies organizational incident response team members to the external providers.

Enhancement Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

References: None.

Priority and Baseline Allocation:

P3	**LOW** IR-7	**MOD** IR-7 (1) **(2)**	**HIGH** IR-7 (1) **(2)**

IR-8 INCIDENT RESPONSE PLAN

Applicability: All Information Systems

Control: The organization:

a. Develops an incident response plan that:
   - Provides the organization with a roadmap for implementing its incident response capability;
   - Describes the structure and organization of the incident response capability;
   - Provides a high-level approach for how the incident response capability fits into the overall organization;
   - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   - Defines reportable incidents;
   - Provides metrics for measuring the incident response capability within the organization;
   - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   - Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*];
c. Reviews the incident response plan at least annually;
d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.

Control Enhancements: None.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-8	**MOD** IR-8	**HIGH** IR-8